

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## **IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

---



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/748,441	12/27/2000	Wolfgang Daum	9D-HR-19614-Daum et al	4179

7590 08/06/2004

John S. Beulick  
Armstrong Teasdale LLP  
ONE METROPOLITAN SQUARE  
SUITE 2600  
ST. LOUIS, MO 63102

EXAMINER

DINH, MINH

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 08/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

**Application No.**

09/748,441

**Applicant(s)**

DAUM ET AL.

**Examiner**

Minh Dinh

**Art Unit**

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) 1-15 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 16-20 and 23-31 is/are rejected.
- 7) ☒ Claim(s) 21 and 22 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on 27 December 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |   |  |
|---|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)            |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>12/31/2001</u> . | 6) <input type="checkbox"/> Other: ____  |

## DETAILED ACTION

### *Election/Restrictions*

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:
  - I. Claims 1-15, drawn to a method for updating keys, classified in class 380, subclass 44.
  - II. Claims 16-31, drawn to a method for authenticating messages, classified in class 713, subclass 170.

The inventions are distinct, each from the other because of the following reasons:

Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention II has separate utility such as key generation. See MPEP § 806.05(d).

2. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.
3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

4. Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Group II, restriction for examination purposes as indicated is proper.

5. During a telephone conversation with Tom Fisher on 7/16/2004 a provisional election was made with traverse to prosecute the invention of Group II, claims 16-31. Affirmation of this election must be made by applicant in replying to this Office action. Claims 1-15 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

6. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 16-19, 23-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sharrow (6,061,668) in view of Menezes ("Handbook of Applied Cryptography").

a. Regarding claim 16, Sharrow discloses a method for authenticating appliance messages in an appliance communication network, the method comprising:

applying at an appliance communication center an appliance message to an algorithm to generate a checksum value (fig. 2); the checksum value meets the limitation of a first authentication word (see specification, p. 23, lines 1-2); and transmitting the appliance message and the first authentication word as an authenticated message to the appliance (fig. 2).

Sharrow does not disclose maintaining at the appliance communication center a shared message counter, the shared message counter shared between the communication center and a remotely located appliance; and applying both the appliance message and the shared message counter to the authentication algorithm to generate the first authentication word. Menezes discloses a method for using sequence numbers in a strong authentication protocol. The Menezes method includes, among other steps, maintaining a shared message counter at both ends of a communication channel, the shared message counter shared between the pair of entities; and assigning a value obtained from the shared message counter to a message to be transmitted (p. 399, see (ii) Sequence numbers and 10.13 Remark). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Menezes method of utilizing sequence numbers into the method of

Art Unit: 2132

Sharrow; in particular, it would have been obvious to one of ordinary skill in the art at the time the invention was made to maintain at the appliance communication center a shared message counter, the shared message counter shared between the communication center and a remotely located appliance; and assign a value obtained from the shared message counter to the appliance message, as taught by Menezes. Accordingly, both the appliance message and the shared message counter are used to generate the first authentication word. The motivation for doing so would have been to detect message replay.

b. Regarding claim 17, Sharrow further discloses receiving the authenticated message at the appliance; applying the appliance message to the authentication algorithm to generate a second authentication word; and comparing the first authentication word and the second authentication word to determine the authenticity of the authenticated message (fig. 2; col. 3, lines 23-26). Menezes further discloses using the shared message counter, as stored in the receiving side, for authentication (p. 399, see (ii) Sequence numbers and 10.13 Remark).

c. Regarding claim 18, Menezes further discloses incrementing the shared message counter, as stored in the receiving side, after receiving a genuine authenticated message at the receiving side (p. 399, see (ii) Sequence numbers and 10.13 Remark).

d. Regarding claim 19, Sharrow does not disclose using an authentication keying variable. Menezes discloses using a random number in combination with a sequence number, the random number meets the limitation of an authentication keying variable (p.

Art Unit: 2132

398, "Combinations of time-variant parameters ... or sequence numbers."). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of claim 16 further to use an authentication keying variable, as taught by Menezes. Accordingly, the authentication keying variable is used to generate the first authentication word. The motivation for doing so would have been to guarantee that a pseudorandom number is not duplicated.

e. Regarding claim 23, Sharrow and Menezes do not disclose maintaining a separate shared counter for a plurality of appliances. However, Sharrow discloses that the appliance communication center communicates with a plurality of appliances (fig. 1) and Menezes discloses that the sequence numbers are specific to a particular pair of entities (p. 399, see (ii) Sequence numbers and 10.13 Remark). Therefore, the feature is obvious by the combination of Sharrow and Menezes discussed in claim 16.

f. Regarding claim 24, Menezes further discloses incrementing the shared message counter, as stored in the sending side, after transmitting the authenticated message (p. 399, see (ii) Sequence numbers and 10.13 Remark).

g. Claims 25-26 are rejected on the same basis as claim 23.

h. Regarding claim 27, Menezes further discloses incrementing the shared message counter, as stored in the sending side, after transmitting the authenticated message (p. 399, see (ii) Sequence numbers and 10.13 Remark).

i. Claim 28 is rejected on the same basis as claim 17.

j. Claim 29 is rejected on the same basis as claim 18.



k. Regarding claim 30, Sharrow discloses a method for authenticating appliance messages, the method comprising:

applying an appliance message to an algorithm to generate a checksum value (fig. 3); the checksum value meets the limitation of a first authentication word (see specification, p. 23, lines 1-2); and

transmitting the appliance message and the first authentication word as an authenticated message to an appliance communication center (fig. 3).

Sharrow does not disclose maintaining at the appliance a shared message counter, the shared message counter shared between the appliance and the appliance communication center; and applying both the appliance message and the shared message counter to the authentication algorithm to generate the first authentication word. Menezes discloses a method for using sequence numbers in a strong authentication protocol. The Menezes method includes, among other steps, maintaining a shared message counter at both ends of a communication channel, the shared message counter shared between the pair of entities; and assigning a value obtained from the shared message counter to a message to be transmitted (p. 399, see (ii) Sequence numbers and 10.13 Remark). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Menezes method of utilizing sequence numbers into the method of Sharrow; in particular, it would have been obvious to one of ordinary skill in the art at the time the invention was made to maintain at the appliance a shared message counter, the shared message counter shared between the appliance and the appliance communication center; and assign a

value obtained from the shared message counter to the appliance message, as taught by Menezes. Accordingly, both the appliance message and the shared message counter are used to generate the first authentication word. The motivation for doing so would have been to detect message replay.

I. Regarding claim 31 Sharrow further discloses receiving the authenticated message at the appliance communication center; applying the appliance message to the authentication algorithm to generate a second authentication word; and comparing the first authentication word and the second authentication word to determine the authenticity of the authenticated message (fig. 2; col. 3, lines 23-26). Menezes further discloses using the shared message counter, as stored in the receiving side, for authentication (p. 399, see (ii) Sequence numbers and 10.13 Remark).

9. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sharrow in view of Menezes as applied to claim 19 above, and further in view of Kaufman et al. ("Network Security Private Communication in a Public World"). Sharrow and Menezes disclose using a shared message counter to generate the first authentication word in claim 16. Sharrow discloses that the authentication algorithm iteratively performs arithmetic or logical operations (col. 3, lines 21-22).

Sharrow and Menezes do not disclose using a directional code to generate the first authentication word. Kaufman teaches using a directional code for authentication (Section 9.3.5 Privacy and Integrity, p. 242, 3<sup>rd</sup> par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined

Art Unit: 2132

method of Sharrow and Menezes to use a directional code for authentication, as taught by Kaufman. Accordingly, the directional code is used to generate the first authentication word. The motivation for doing so would have been to be able to prevent a reflection attack.

Sharrow discloses a working register (col. 5, lines 1-5). Sharrow does not disclose that the working register comprising at least four bytes, the first three bytes holding the shared message counter and the fourth byte holding the directional code.

However, these limitations are considered design choices because they provide no criticality to the invention. *The differences between the working register as claimed to and the working register of Sharrow is a matter of design choice since both store the counter and directional code.*

**Allowable Subject Matter**

10. Claims 21-22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

11. The following is a statement of reasons for the indication of allowable subject matter. Regarding claim 21, the limitations "forming P as the dot product of R2 and R0; forming Q as the bitwise exclusive or of P with the constant expression '01010101'; forming S by adding Q to K; forming S' by end around rotating S; forming T as the bitwise exclusive or of S' and R3; forming F as the bitwise exclusive or of T with a byte of the appliance message; and replacing R3 with R2, R2 with R1, R1 with R0, and R0

with F", in combination with elements of the parent claims, have not been taught by prior art.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

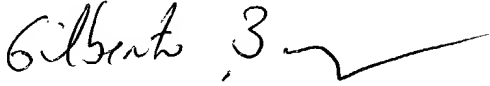
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh  
Examiner  
Art Unit 2132

MD  
7/26/2004

  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100